PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-005644

(43)Date of publication of application : 08.01.2003

(51)Int.Cl. G09C 1/00

(21)Application number : 2002-089675

(22)Date of filing : 27.03.2002

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(72)Inventor : FUDA YUICHI
ONO TAKATOSHI
OMORI MOTOJI

(30)Priority

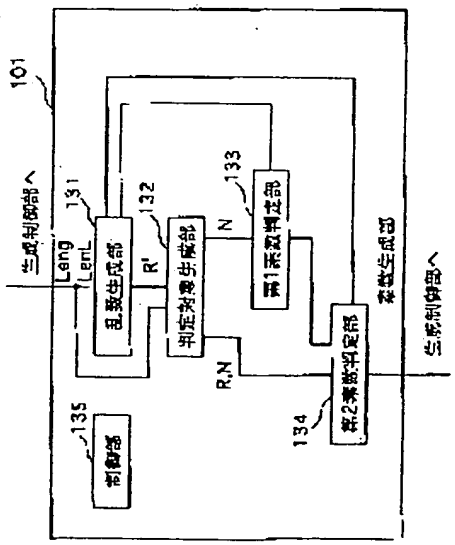
Priority number : 2001117842 Priority date : 17.04.2001 Priority country : JP

(54) INFORMATION SECURITY APPARATUS, APPARATUS AND METHOD FOR GENERATING PRIME NUMBER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a prime number generating apparatus which can reduce a quantity of calculation and definitely generate prime numbers.

SOLUTION: An information security apparatus inputs a prime number q and generates a prime number N greater than q and is provided with a partial information setting part, a random number generating part, a part for generating an object to be determined and a part for determining the prime number. The partial information setting part generates the number u meeting a formula 2 ×u×q+1≠0 mod Li (i=1, 2,..., n). The random number generating part generates a random number R'. The part for generating the object to be determined generates R=u+L1×L2×...×Ln×R' and N=2×R×q+1 by using the number u and the random number R'. The part for determining the prime number determines the prime number by using the numbers N and R.



LEGAL STATUS

[Date of request for examination]	13.12.2004
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－5644
（P2003－5644A）
(43)公開日　平成15年１月８日(2003.1.8)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｇ０９Ｃ　1/00	６５０ ６６０	Ｇ０９Ｃ　1/00	６５０Ｚ　５Ｊ１０４ ６６０Ａ

審査請求　未請求　請求項の数12　ＯＬ　（全 20 頁）

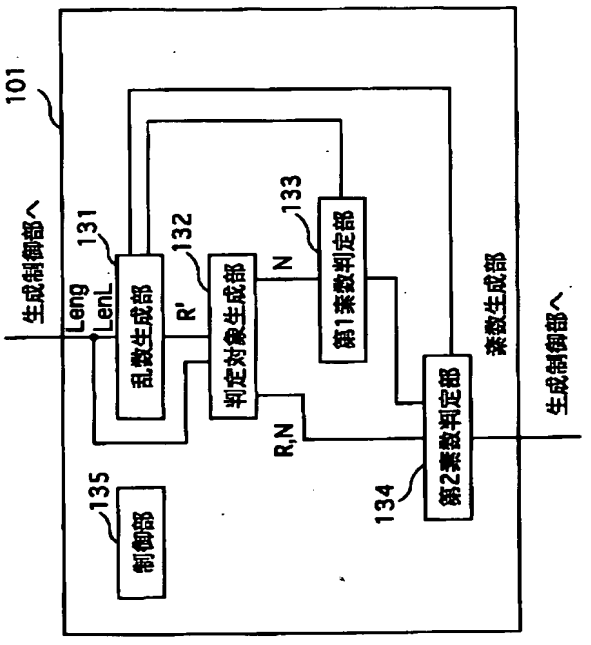
(21)出願番号　特願2002－89675(P2002－89675)
(22)出願日　平成14年３月27日(2002.3.27)
(31)優先権主張番号　特願2001－117842(P2001－117842)
(32)優先日　平成13年４月17日(2001.4.17)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　布田　裕一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　小野　貴敏
愛知県名古屋市中区栄２丁目６番１号　白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　情報セキュリティ装置、素数生成装置及び素数生成方法

(57)【要約】
【課題】　計算量が少なく、かつ、確定的に素数生成が可能な素数生成装置を提供する。
【解決手段】情報セキュリティ装置は、素数ｑを入力とし、ｑより大きな素数Ｎを生成する。２×ｕ×ｑ＋１≠０　ｍｏｄ　L_i　（ｉ＝１、２、・・・、ｎ）を満たす数ｕを生成する部分情報設定部と、乱数Ｒ’を生成する乱数生成部と、数ｕと、乱数Ｒ’を用いて、Ｒ＝ｕ＋$L_1 \times L_2 \times \cdots \times L_n \times R'$と、Ｎ＝２×Ｒ×ｑ＋１を生成する判定対象生成部と、数Ｎ及び数Ｒを用いて素数判定する素数判定部を備える。



1

【特許請求の範囲】

【請求項１】　素因数分解をすることが計算量の上で困難であることを根拠として、２個の素数を生成し生成した２個の素数の乗算を用いて、所定の情報を安全かつ確実に扱い、各素数生成の際に、既知の素数ｑの２倍のビット長を有する素数Ｎを生成する情報セキュリティ装置であって、

素数ｑ及びｎ個の素数L_1、L_2、・・・、L_nを取得し、ここで、素数L_1、L_2、・・・、L_nは、それぞれ素数ｑより小さい２以外の素数であり、素数ｑは、

$q=1 \mod L_i$　（ｉ＝１、２、・・・、ｎ）　を満たす取得手段と、

取得した前記素数L_1、L_2、・・・、L_nに係る数を除外した選択により、取得した前記素数ｑの２倍のビット長を有する数Ｎを生成する生成手段と、生成した数Ｎの素数判定を行い、数Ｎが素数であると判定とされた場合に、数Ｎを素数として出力する判定手段とを備えることを特徴とする情報セキュリティ装置。

【請求項２】　前記生成手段は、

$N=1 \mod L_i$　（ｉ＝１、２、・・・、ｎ）　を満たす前記数Ｎを生成することを特徴とする請求項１に記載の情報セキュリティ装置。

【請求項３】　前記生成手段は、

（ＬｅｎｑーＬｅｎＬ－１）ビット長の乱数Ｒ’を生成し、ここで、Ｌｅｎｑは、素数ｑのビット長であり、ＬｅｎＬは、（$L_1 \times L_2 \times \cdots \times L_n$）のビット長である乱数生成部と、

生成したＲ’及び前記素数L_1、L_2、・・・、L_nを用いて、数$R=L_1 \times L_2 \times \cdots \times L_n \times R'$により、数Ｒを生成し、取得した素数ｑ及び生成した数Ｒを用いて、数Ｎ＝２×Ｒ×ｑ＋１を生成する判定対象生成部とを含み、

前記判定手段は、前記数Ｎ及び前記数Ｒを用いて、前記数Ｎの素数判定を行うことを特徴とする請求項２に記載の情報セキュリティ装置。

【請求項４】　前記判定手段は、生成した前記数Ｎについて、

第１判定式　$2^{N-1}=1 \mod N$

が成立するか否かを判定し、

さらに、生成した前記数Ｎ及び前記数Ｒについて、

第２判定式　$2^{2R} \neq 1 \mod N$

が判定するか否かを判定し、

第１判定式及び第２判定式の両方が成立する場合に、数Ｎが素数であると判定することを特徴とする請求項３に記載の情報セキュリティ装置。

【請求項５】　前記生成手段は、

取得した前記素数ｑを用いて、

$2 \times u \times q + 1 \neq 0 \mod L_i$　（ｉ＝１、２、・・・、ｎ）

を満たす数ｕを生成する部分情報生成部と、

2

乱数Ｒ’を生成する乱数生成部と、

取得した前記素数L_1、L_2、・・・、L_nと、生成した前記数ｕと、生成した前記乱数Ｒ’を用いて、

$R=u+L_1 \times L_2 \times \cdots \times L_n \times R'$

により、数Ｒを生成し、取得した前記素数ｑと、生成した数Ｒとを用いて、

$N=2 \times R \times q + 1$

により、数Ｎを生成する判定対象生成部とを含み、

前記判定手段は、前記数Ｎ及び前記数Ｒを用いて、前記数Ｎの素数判定を行うことを特徴とする請求項１に記載の情報セキュリティ装置。

【請求項６】　前記部分情報生成部は、

整数N_1　（$1 \leqq N_1 \leqq L_1 - 1$）、整数$N_2$　（$1 \leqq N_2 \leqq L_2 - 1$）、・・・、

整数N_n　（$1 \leqq N_n \leqq L_n - 1$）を生成し、

数$u_i = (N_i - 1) / (2 \times (q \mod L_i)) \mod L_i$　（ｉ＝１、２、・・・、ｎ）

を算出する整数生成部と、

算出した前記数u_i　（ｉ＝１、２、・・・、ｎ）を用いて、

数$u = u_i \mod L_i$　（ｉ＝１、２、・・・、ｎ）

を満たす数ｕを算出する情報合成部とを含むことを特徴とする請求項５に記載の情報セキュリティ装置。

【請求項７】　前記判定手段は、生成した前記数Ｎについて、

第１判定式　$2^{N-1}=1 \mod N$

が成立するか否かを判定し、

さらに、生成した前記数Ｎ及び前記数Ｒについて、

第２判定式　$2^{2R} \neq 1 \mod N$

が判定するか否かを判定し、

第１判定式及び第２判定式の両方が成立する場合に、数Ｎが素数であると判定することを特徴とする請求項６に記載の情報セキュリティ装置。

【請求項８】　素因数分解をすることが計算量の上で困難であることを根拠として、２個の素数を生成し生成した２個の素数の乗算を用いて、所定の情報を安全かつ確実に扱い、各素数生成の際に、既知の素数ｑの２倍のビット長を有する素数Ｎを生成するＩＣカードであって、

素数ｑ及びｎ個の素数L_1、L_2、・・・、L_nを取得し、ここで、素数L_1、L_2、・・・、L_nは、それぞれ素数ｑより小さい２以外の素数であり、素数ｑは、

$q=1 \mod L_i$　（ｉ＝１、２、・・・、ｎ）　を満たす取得手段と、

取得した前記素数L_1、L_2、・・・、L_nに係る数を除外した選択により、取得した前記素数ｑの２倍のビット長を有する数Ｎを生成する生成手段と、

生成した数Ｎの素数判定を行い、数Ｎが素数であると判定とされた場合に、数Ｎを素数として出力する判定手段とを備えることを特徴とするＩＣカード。

【請求項９】　既知の素数ｑの２倍のビット長を有する

素数Ｎを生成する素数生成装置であって、
素数ｑ及びｎ個の素数L_1、L_2、・・・、L_nを取得し、ここで、素数L_1、L_2、・・・、L_nは、それぞれ素数ｑより小さい２以外の素数であり、素数ｑは、
$q=1 \mod L_i$　（ｉ＝１、２、・・・、ｎ）　を満たす取得手段と、
取得した前記素数L_1、L_2、・・・、L_nに係る数を除外した選択により、取得した前記素数ｑの２倍のビット長を有する数Ｎを生成する生成手段と、
生成した数Ｎの素数判定を行い、数Ｎが素数であると判定とされた場合に、数Ｎを素数として出力する判定手段とを備えることを特徴とする素数生成装置。
【請求項１０】　既知の素数ｑの２倍のビット長を有する素数Ｎを生成する素数生成装置で用いられる素数生成方法であって、
素数ｑ及びｎ個の素数L_1、L_2、・・・、L_nを取得し、ここで、素数L_1、L_2、・・・、L_nは、それぞれ素数ｑより小さい２以外の素数であり、素数ｑは、
$q=1 \mod L_i$　（ｉ＝１、２、・・・、ｎ）　を満たす取得ステップと、
取得した前記素数L_1、L_2、・・・、L_nに係る数を除外した選択により、取得した前記素数ｑの２倍のビット長を有する数Ｎを生成する生成ステップと、
生成した数Ｎの素数判定を行い、数Ｎが素数であると判定とされた場合に、数Ｎを素数として出力する判定ステップとを含むことを特徴とする素数生成方法。
【請求項１１】　既知の素数ｑの２倍のビット長を有する素数Ｎを生成するコンピュータで用いられる素数生成プログラムであって、
素数ｑ及びｎ個の素数L_1、L_2、・・・、L_nを取得し、ここで、素数L_1、L_2、・・・、L_nは、それぞれ素数ｑより小さい２以外の素数であり、素数ｑは、
$q=1 \mod L_i$　（ｉ＝１、２、・・・、ｎ）　を満たす取得ステップと、
取得した前記素数L_1、L_2、・・・、L_nに係る数を除外した選択により、取得した前記素数ｑの２倍のビット長を有する数Ｎを生成する生成ステップと、
生成した数Ｎの素数判定を行い、数Ｎが素数であると判定とされた場合に、数Ｎを素数として出力する判定ステップとを含むことを特徴とする素数生成プログラム。
【請求項１２】　既知の素数ｑの２倍のビット長を有する素数Ｎを生成するコンピュータで用いられる素数生成プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記素数生成プログラムは、
素数ｑ及びｎ個の素数L_1、L_2、・・・、L_nを取得し、ここで、素数L_1、L_2、・・・、L_nは、それぞれ素数ｑより小さい２以外の素数であり、素数ｑは、
$q=1 \mod L_i$　（ｉ＝１、２、・・・、ｎ）　を満たす取得ステップと、

取得した前記素数L_1、L_2、・・・、L_nに係る数を除外した選択により、取得した前記素数ｑの２倍のビット長を有する数Ｎを生成する生成ステップと、
生成した数Ｎの素数判定を行い、数Ｎが素数であると判定とされた場合に、数Ｎを素数として出力する判定ステップとを含むことを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、素数生成を用いて実現する情報セキュリテイ技術に関する。
【０００２】
【従来の技術】近年、コンピュータ技術及び通信技術に基づくデータ通信が広く普及してきており、このデータ通信においては、秘密通信方式やデジタル署名方式が用いられる。ここで、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、発信者の身元を証明する通信方式である。
【０００３】１．公開鍵暗号方式
これらの秘密通信方式又はデジタル署名方式においては、公開鍵暗号方式とよばれる暗号方式が用いられる。公開鍵暗号方式は通信相手が多数のとき、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。公開鍵暗号方式を用いる秘密通信では、暗号化鍵と復号化鍵とが異なり、復号化鍵は秘密にするが、暗号化鍵は公開する。秘密にする復号化鍵を秘密鍵と呼び、公開する暗号化鍵を公開鍵と呼ぶ。
【０００４】公開鍵暗号方式の１種であるＲＳＡ暗号方式では、整数の素因数分解問題を解くことが、計算量の上で困難であることを安全性の根拠としている。素因数分解問題とは、ｐ、ｑを素数とし、整数ｎ＝ｐ×ｑとするとき、整数ｎに対して、素数ｐ、ｑを求める問題である。ここで、×は通常の乗算である。なお、素因数分解問題については、岡本龍明、太田和夫共編、「暗号・ゼロ知識問題・数論」、共立出版、１９９０、１４４～１５１ページに詳しく述べられている。
【０００５】（素因数分解問題を応用するＲＳＡ暗号方式）素因数分解問題を応用するＲＳＡ暗号方式について説明する。
（１）鍵の生成
次に示すようにして公開鍵及び秘密鍵を計算する。
・ランダムに大きい素数ｐ、ｑを選択し、その積ｎ＝ｐ×ｑを計算する。
【０００６】・（ｐ－１）及び（ｑ－１）の最小公倍数Ｌ＝ＬＣＭ（ｐ－１、ｑ－１）を計算する。
・Ｌと互いに素でＬより小さい整数ｅをランダムに選ぶ。
$1 \leqq e \leqq L-1$、ＧＣＤ（ｅ、Ｌ）＝１

5

ここで、ＧＣＤ（ｅ、Ｌ）は、ｅ及びＬの最大公約数を示している。

【０００７】・ｄ＝e^{-1}　ｍｏｄ　Ｌを計算する。このようにして、得られた整数ｅ及び整数ｎが、公開鍵である。また、整数ｄが、秘密鍵である。

（２）暗号文の生成

公開鍵である整数ｅ及び整数ｎを用いて、平文ｍに暗号演算を施して暗号文ｃを計算する。

【０００８】ｃ＝m^{e}　ｍｏｄ　ｎ

（３）復号文の生成

秘密鍵である整数ｄを用いて、暗号文ｃに復号演算を施して復号文ｍ’を計算する。

ｍ’＝c^{d}　ｍｏｄ　ｎ

なお、

ｍ’＝c^{d}　ｍｏｄ　ｎ

＝$(m^{e})^{d}$　ｍｏｄ　ｎ

＝ｍ＊＊（ｅ×ｄ　ｍｏｄ　Ｌ）　ｍｏｄ　ｎ

＝m^{1}　ｍｏｄ　ｎ

＝ｍ　ｍｏｄ　ｎ

であるので、復号文ｍ’は、平文ｍと一致する。

【０００９】なお、この明細書において、演算子＊＊は、べき乗を示す。例えば、Ａ＊＊ｘは、A^{x}であり、ＡをＸ回乗ずることを示す。また、ＲＳＡ暗号については、岡本龍明、山本博資、「現代暗号」、産業図書、１９９７、１１０～１１３ページに詳しく説明されている。

２．従来例１－確率的素数生成方法

上記に示した素因数分解を応用したＲＳＡ暗号における公開鍵の生成のステップにおいて、素数生成が行われる。素数生成については、A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, “Handbook of applied cryptography”, CRC Press, 1997, 145～154ページに詳しく説明されている。

【００１０】従来技術としての確率的素数生成方法について、説明する。この確率的素数生成方法は、素数判定法であるMiller-Rabin法を応用している。Miller-Rabin法については、A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, “Handbook ofapplied cryptography”, CRC Press, 1997, 138～140ページに詳しく説明されている。この素数判定法による判定される素数は、「素数である確率が高い」数であり、１００％素数であるとは限らないということを注意しておく。

【００１１】あらかじめ自然数ｘと、小さい素数L_1、L_2、・・・、L_nとが与えられているものとする。ここで、小さい素数の一例は、「２、３、５、７」である。前記確率的素数生成方法では、次に示すステップを繰り返すことにより、素数を生成する。

（ステップ１）初期値として、自然数ｘを変数Ｎに代入する。

【００１２】（ステップ２）変数Ｎより大きい数のうち、素数L_1、L_2、・・・、L_nのいずれでも割り切れない数であって、最も小さい数を得、得られた数を変数Ｎに代入する。

（ステップ３）Miller-Rabin法により変数Ｎの値が素数であるか否かを判定する。ここで、変数Ｎに対して素数判定を１０回繰り返す。判定の結果、素数であると判定される場合には、変数Ｎの値を素数として出力する。素数でないと判定される場合には、ステップ２へ戻って、素数が出力されるまで、処理を繰り返す。

【００１３】上記のように、小さい素数２、３、５、７で割り切れない数を求める理由は、ステップ３の素数判定の回数を減らすためである。即ち、素数判定する対象となる数を２、３、５、７で割り切れない数だけに絞っている。２×ｘ＋１　ｍｏｄ２１０が２、３、５、７で割り切れない数は４７個あるため、上記のように、２、３、５、７で割り切れない数のみを対象として素数判定すると、素数判定する回数は、４７／２１０に削減できる。

【００１４】しかしながら、ステップ２により得られた変数Ｎの値が合成数（素数でない数）であるとき、Miller-Rabin法による素数判定が成立する確率は、１／４以下であることが知られている。このように、得られた変数Ｎの値が合成数であっても、Miller-Rabin法による素数判定が成立する可能性がある。そのため、前記確率的素数生成方法は、確率的にのみ素数を生成でき、確定的に素数を生成できないという問題がある。

【００１５】（確率的素数生成方法の計算量）次に、前記確率的素数生成方法を用いて素数を生成する場合の計算量について説明する。ここでは、冪乗剰余演算の回数で計算量を見積もるものとする。前記確率的素数生成方法では、上述したように、素数と思われる数に対しては、Miller-Rabin法による素数判定を１０回繰り返す。以下では、合成数に対して行われるMiller-Rabin法による素数判定の回数の平均を求める。

【００１６】第ｉ回目の素数判定試行を行う確率をP_iとすると、第ｉ＋１回目の素数判定試行を行う確率P_{i+1}は、第ｉ回のP_iの確率で素数判定試行を行い、かつ１／４以下の確率でさらに素数判定試行を行う確率である。従って、

$P_{i+1} \leqq P_i \times 1/4$

である。第１回目の素数判定試行は、必ず行うため、その確率は１であるので、$P_1 = 1$である。よって、

$P_i \leqq (1/4)^{**}(i-1)$

である。

【００１７】Miller-Rabin法による素数判定１回につき、冪乗剰余演算を１回行う。前記確率的素数生成方法では、Miller-Rabin法による素数判定を最大で１０回行うため、１つの合成数に対する冪乗剰余演算回数の平均値は、

【００１８】

7

【数１】

$$\sum_{i=1}^{10} P_i \leq \sum_{i=1}^{10} (1/4) ** (i-1) = 1.33$$

【００１９】である。一般にＮを任意に選ぶとき、Ｎが素数となる確率は、１／（ｌｎ　Ｎ）程度であるので、平均的には、ｌｎ　Ｎ回の素数判定を行うと素数を発見できることになる。ここで、ｌｎ　Ｎは、Ｎの自然対数である。しかし、２、３、５、７で割り切れる数は予め除外しているので、その回数は、φ（２×３×５×７）／２１０＝４８／２１０に削減できる。ここで、φ（２×３×５×７）は、２１０未満の自然数の２、３、５、＊７と互いに素な数の個数を示している。従って、素数判定を行う数（合成数と最後の素数と思われる数）の個数は、

８／３５×（ｌｎ　Ｎ）

である。その中で、最後の数が素数であると考えると、素数判定を行う合成数の個数は、

（８／３５×（ｌｎ　Ｎ））－１

となる。

【００２０】以上より、冪乗剰余演算の回数は、平均的に、

【００２１】

【数２】

$$(8/35 \times (\ln N) - 1) \times \left(\sum_{i=1}^{10} 1/(4 ** (n-1))\right) + 10$$

【００２２】以下である。例えば、Ｎが５１２ビットのとき、多くとも１１６．８回であることが保証されている。素数判定を行う数を２、３、５、７で割り切れない数に絞り込まない場合、即ち、全ての数を素数判定を行う対象にする場合、冪乗剰余演算の回数は、平均的に、

【００２３】

【数３】

$$(\ln N - 1) \times \left(\sum_{i=1}^{10} 1/(4 ** (n-1))\right) + 10$$

【００２４】以下である。Ｎが５１２ビットのとき、この値は４８１．９になる。以上より、従来例１は、冪乗剰余演算回数が約１／４に削減できる。しかしながら、上述したように、確定的に素数を出力できない。

３．従来例２－確定的素数生成方法

確定的に素数を生成することができるＭａｕｒｅｒ法による確定的素数生成方法について説明する。ここで、Ｍａｕｒｅｒ法については、A.J. Menezes, P.C.van Oorschot, S.A. Vanstone, “Handbook of applied cryptography”, CRCPress, 1997, 152～153ページに詳しく説明されている。

【００２５】前記確定的素数生成方法では、次に示すステップを繰り返すことにより、素数を生成する。あらかじめサイズＬｅｎｑの素数ｑが与えられている。

（ステップ１）Ｌｅｎｑ－１ビットの乱数Ｒを選択する。なお、乱数Ｒの先頭ビットは、必ず１となるようにする。

【００２６】（ステップ２）数Ｎを以下の式により計算する。

Ｎ＝２×ｑ×Ｒ＋１

（ステップ３）数Ｎが素数であるか否かを、次に示す第１判定及び第２判定がともに、成立する場合に、素数と判定する。他の場合に、素数でないと判定する。

【００２７】

（第１判定）　$2^{N-1} = 1 \mod N$

（第２判定）　$GCD(2^{2R} - 1, N) = 1$

素数であると判定される場合には、数Ｎを素数として出力する。素数でないと判定される場合には、ステップ１へ戻って、素数が出力されるまで、処理を繰り返す。

【００２８】この判定方法は、Pocklingtonの素数判定法とよばれ、A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, “Handbook of applied cryptography”, CRC Press, 1997, 144ページに詳しく述べられている。Pocklington の素数判定法では、Ｎ＝２×ｑ×Ｒ＋１のｑが素数であり、第１判定及び第２判定の結果が真であれば、必ず、Ｎが素数になる。そのため、確定的に素数であることを判定でき、確定的な素数生成が可能になる。

【００２９】このようにして、Ｍａｕｒｅｒ法による確定的素数生成方法では、サイズＬｅｎｑの素数ｑを基にして、サイズ２×Ｌｅｎｑの素数Ｎを生成する。従って、Ｍａｕｒｅｒ法による確定的素数生成方法を用いて所定長の素数を生成する場合には、前記所定長以下の素数の生成を繰り返し行う。例えば、５１２ビット長の素数を生成する場合には、あらかじめ与えられた８ビットの素数を基にして１６ビットの素数を生成する。次に、生成した１６ビットの素数を基にして３２ビットの素数

を生成する。次に、生成した３２ビットの素数を基にして６４ビットの素数を生成する。以下同様の素数生成を繰り返して、５１２ビットの素数を生成する。

【００３０】なお、前記第２判定を次の判定に代えてもよい。

$2^{2^R} \neq 1 \mod N$

（確定的素数生成方法の計算量）次に、Ｍａｕｒｅｒ法による確定的素数生成方法を用いて素数を生成する場合の計算量について説明する。

【００３１】ここでは、５１２ビットの数の冪乗剰余演算の回数で計算量を見積もる。つまり、２５６ビットの素数を用いて、５１２ビットの素数を生成する場合について考える。一般に、正整数Ｒを任意に選ぶとき、正整数Ｒが素数となる確率は、１／（ｌｎ　Ｒ）程度であるので、この場合、５１２ビットの素数を生成するためにPocklington 判定を試す回数は、$\ln 2^{512}$ と見積もることができる。従来例２では奇数のみに対して、素数判定を行うので、この個数は、$(\ln 2^{512})/2$ となる。

【００３２】次に、前記第１判定を通過する確率は、Miller-Rabin判定を通過する確率と等しく、１／４以下である。従って、１つの合成数に対して行う冪乗剰余演算の回数は、１＋１／４以下である。当然、素数に対して行う冪乗剰余演算回数は、２である。以上より、２５６ビットの素数を用いて、５１２ビットの素数を生成するために行う５１２ビットの冪乗剰余演算回数は、

$(1+1/4)((\ln 2^{512})/2-1)+2=222.6$

以下である。

【００３３】１２８ビットから２５６ビットの素数を生成する場合も同様に考えると、２５６ビットの冪乗剰余演算における判定回数は、$(\ln 2^{256})/2$ であり、２５６ビットの素数を生成するために行う２５６ビットの冪乗剰余演算回数は、

$(1+1/4)((\ln 2^{256})/2-1)+2$

以下である。冪乗剰余演算の計算量は、法Ｎに依存し、Ｎの３乗のオーダである。従って、２５６ビットの冪乗剰余演算８回を、５１２ビットの冪乗剰余演算１回相当と考える。

【００３４】６４ビットから１２８ビットなどの他も同様に考えると、従来例２全体の計算量を、５１２ビットの冪乗剰余演算回数で見積もることができる。１６、３２ビットの素数生成の計算量は、６４、１２８、２５６、５１２ビットの素数生成の計算量に比べて小さいため無視し、従来例２全体の計算量を、５１２ビットの冪乗剰余演算回数で表すと、

$(1+1/4)\times\{((\ln 2^{64})/2-1)/512+((\ln 2^{128})/2-1)/64+((\ln 2^{256})/2-1)/8+((\ln 2^{512})/2-1)\}+2$

$(1/512+1/64+1/8+1)=237.4$

以下である。

【００３５】従来例２における計算量は、従来例１の１１６．８回以下に比べれば、計算量が２倍以上多いことになる。以上説明したように、従来例２によると、確定的な素数生成が可能であるが、従来例１より計算量が多い。

【００３６】

【発明が解決しようとする課題】このように、計算量が少ない素数生成法では、確定的に素数生成ができないという問題がある。また、確定的に素数生成が可能な素数法では、計算量が多いという問題がある。本発明は、上記の問題点を解決し、計算量が少なく、かつ、確定的に素数生成が可能な素数生成装置、素数生成方法、素数生成プログラム、素数生成プログラムを記録している記録媒体及び情報セキュリティ装置を提供することを目的とする。

【００３７】

【課題を解決するための手段】上記目的を達成するために、本発明は、素因数分解をすることが計算量の上で困難であることを根拠として、２個の素数を生成し生成した２個の素数の乗算を用いて、所定の情報を安全かつ確実に扱い、各素数生成の際に、既知の素数ｑの２倍のビット長を有する素数Ｎを生成する情報セキュリティ装置であって、素数ｑ及びｎ個の素数L_1、L_2、・・・、L_nを取得し、ここで、素数L_1、L_2、・・・、L_nは、それぞれ素数ｑより小さい２以外の素数であり、素数ｑは、$q=1 \mod L_i$（ｉ＝１、２、・・・、ｎ）を満たす取得手段と、取得した前記素数L_1、L_2、・・・、L_nに係る数を除外した選択により、取得した前記素数ｑの２倍のビット長を有する数Ｎを生成する生成手段と、生成した数Ｎの素数判定を行い、数Ｎが素数であると判定とされた場合に、数Ｎを素数として出力する判定手段とを備える。

【００３８】ここで、前記生成手段は、$N=1 \mod L_i$（ｉ＝１、２、・・・、ｎ）を満たす前記数Ｎを生成するように構成してもよい。ここで、前記生成手段は、（ＬｅｎｑーＬｅｎＬ－１）ビット長の乱数Ｒ’を生成し、ここで、Ｌｅｎｑは、素数ｑのビット長であり、ＬｅｎＬは、$(L_1\times L_2\times\cdots\times L_n)$のビット長である乱数生成部と、生成したＲ’及び前記素数L_1、L_2、・・・、L_nを用いて、数$R=L_1\times L_2\times\cdots\times L_n\times R'$により、数Ｒを生成し、取得した素数ｑ及び生成した数Ｒを用いて、数$N=2\times R\times q+1$を生成する判定対象生成部とを含み、前記判定手段は、前記数Ｎ及び前記数Ｒを用いて、前記数Ｎの素数判定を行うように構成してもよい。

【００３９】ここで、前記判定手段は、生成した前記数Ｎについて、第１判定式 $2^{N-1}=1 \mod N$ が成立するか否かを判定し、さらに、生成した前記数Ｎ及

び前記数Ｒについて、第２判定式　$2^{2R} \neq 1 \mod N$　が判定するか否かを判定し、第１判定式及び第２判定式の両方が成立する場合に、数Ｎが素数であると判定するように構成してもよい。

【００４０】ここで、前記生成手段は、取得した前記素数ｑを用いて、$2 \times u \times q + 1 \neq 0 \mod L_i$　（ｉ＝１、２、・・・、ｎ）　を満たす数ｕを生成する部分情報生成部と、乱数Ｒ’を生成する乱数生成部と、取得した前記素数L_1、L_2、・・・、L_nと、生成した前記数ｕと、生成した前記乱数Ｒ’を用いて、　$R = u + L_1 \times L_2 \times \cdots \times L_n \times R'$により、数Ｒを生成し、取得した前記素数ｑと、生成した数Ｒとを用いて、　$N = 2 \times R \times q + 1$　により、数Ｎを生成する判定対象生成部とを含み、前記判定手段は、前記数Ｎ及び前記数Ｒを用いて、前記数Ｎの素数判定を行うように構成してもよい。

【００４１】ここで、前記部分情報生成部は、整数N_1（$1 \leqq N_1 \leqq L_1 - 1$）、整数$N_2$（$1 \leqq N_2 \leqq L_2 - 1$）、・・・、整数$N_n$（$1 \leqq N_n \leqq L_n - 1$）を生成し、数$u_i = (N_i - 1) / (2 \times (q \mod L_i)) \mod L_i$　（ｉ＝１、２、・・・、ｎ）　を算出する整数生成部と、算出した前記数u_i（ｉ＝１、２、・・・、ｎ）を用いて、数$u = u_i \mod L_i$（ｉ＝１、２、・・・、ｎ）を満たす数ｕを算出する情報合成部とを含むように構成してもよい。

【００４２】

【発明の実施の形態】１．第１の実施の形態

本発明に係る１の実施の形態としてのコンテンツ配信システム１について、説明する。

１．１　コンテンツ配信システム１の構成

コンテンツ配信システム１は、図１に示すように、メモリカード１０、携帯情報端末装置（以下、ＰＤＡと呼ぶ。）２０、ヘッドフォン２１、パーソナルコンピュータ（以下、ＰＣと呼ぶ。）３０、配信サーバ装置４０及び携帯電話５０から構成されている。

【００４３】配信サーバ装置４０は、音楽であるデジタル著作物を暗号化して暗号化デジタル著作物を得、得られた暗号化デジタル著作物を、インターネット６０を介して、ＰＣ３０へ送信し、ＰＣ３０は、暗号化デジタル著作物を受信する。利用者は、メモリカード１０をＰＣ３０に装着し、ＰＣ３０は、受信した暗号化デジタル著作物をメモリカード１０へ書き込む。メモリカード１０は、暗号化デジタル著作物を復号して、デジタル著作物を生成し、生成したデジタル著作物を記憶する。次に、利用者は、暗号化デジタル著作物が書き込まれているメモリカード１０をＰＤＡ２０に装着する。ＰＤＡ２０には、ヘッドフォン２１が接続されており、ＰＤＡ２０は、メモリカード１０に書き込まれているデジタル著作物を変換して電気信号を生成し、生成した電気信号をヘッドフォン２１へ出力する。ヘッドフォン２１は、電気信号を音声に変換して、音声を出力する。

【００４４】また、配信サーバ装置４０は、音楽であるデジタル著作物を暗号化して暗号化デジタル著作物を得、得られた暗号化デジタル著作物を、インターネット６０、携帯電話網６２及び無線基地局６１を介して、携帯電話５０へ送信し、携帯電話５０は、暗号化デジタル著作物を受信する。利用者は、メモリカード１０を携帯電話５０に装着し、携帯電話５０は、受信した暗号化デジタル著作物をメモリカード１０へ書き込む。メモリカード１０は、書き込まれている暗号化デジタル著作物を復号して、音楽であるデジタル著作物を生成して、生成したデジタル著作物を記憶する。携帯電話５０は、メモリカード１０に記憶されているデジタル著作物を変換して電気信号を生成し、生成した電気信号を音声に変換して、音声を出力する。

【００４５】このようにして、利用者は、配信サーバ装置４０から音楽であるデジタル著作物を受信して、楽しむことができる。

１．２　メモリカード１０

メモリカード１０は、図２に示すように、素数生成部１０１、生成制御部１０２、素数記憶部１０３、乱数生成部１０４、秘密鍵記憶部１０５、公開鍵生成部１０６、公開鍵記憶部１０７、復号部１０８、メモリ部１０９、制御部１１２、認証部１１３及び送受信部１１４から構成されている。

【００４６】メモリカード１０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、メモリカード１０は、その機能を達成する。

【００４７】（１）秘密鍵記憶部１０５

秘密鍵記憶部１０５は、秘密鍵としての数ｎと数ｄとを記憶するための領域を備えている。

（２）公開鍵記憶部１０７

公開鍵記憶部１０７は、公開鍵としての数ｎと数ｅとを記憶するための領域を備えている。

【００４８】（３）メモリ部１０９

メモリ部１０９は、一般領域１１１とセキュア領域１１０とから構成されている。一般領域１１１及びセキュア領域１１０は、それぞれ情報を記憶するための領域である。一般領域１１１は、外部からの情報の自由な書き込みと、情報の自由な読み出しが許可される領域である。一方、セキュア領域１１０は、認証部１１３により、メモリカード１０が装着される相手の装置の正当性が認証された場合にのみ、情報の書き込み及び情報の読み出しが許可される領域である。

【００４９】（４）素数記憶部１０３

素数記憶部１０３は、素数p_a及び素数p_bを記憶するための領域を備えている。

（５）生成制御部１０２

生成制御部１０２は、素数生成部１０１へ、素数ｑと、素数ｑのビットサイズＬｅｎｑと、２以外の小さな素数であるL_1、L_2、…、L_nと、（$L_1 \times L_2 \times \cdots \times L_n$）のビットサイズＬｅｎＬとを出力し、次に、素数生成部１０１から１個の素数ｐを受け取り、受け取った素数ｐを素数p_nとして素数記憶部１０３へ書き込む。

【００５０】次に、同様にして、素数生成部１０１へ、素数ｑと、素数ｑのビットサイズＬｅｎｑと、２以外の小さな素数であるL_1、L_2、…、L_nと、（$L_1 \times L_2 \times \cdots \times L_n$）のビットサイズＬｅｎＬとを出力し、次に、素数生成部１０１から１個の素数ｐを受け取り、受け取った素数ｐを素数p_nとして素数記憶部１０３へ書き込む。

【００５１】なお、素数ｑと、素数ｑのビットサイズＬｅｎｑと、２以外の小さな素数であるL_1、L_2、…、L_nと、（$L_1 \times L_2 \times \cdots \times L_n$）のビットサイズＬｅｎＬとについては、後述する。上記に説明しているように、生成制御部１０２は、素数生成部１０１を２回、制御することにより、２個の素数を生成している。後述するように、素数生成部１０１により素数を生成するプロセスにおいて、乱数を用いているので、生成された２個の素数が偶然一致する可能性は、低いと考えられる。しかしながら、生成された２個の素数が偶然一致した場合において、生成制御部１０２は、再度２回目の素数生成をするように、素数生成部１０１を制御し、必ず異なる２個の素数を採用するようにしてもよい。

【００５２】また、生成制御部１０２は、前記２回の素数生成の際に、素数ｑと、ビットサイズＬｅｎｑと、素数L_1、L_2、…、L_nと、ビットサイズＬｅｎＬとからなるパラメタ群を用いるとしているが、２回の素数生成の際に異なるパラメタ群を用いるとしてもよい。つまり、１回めの素数生成の際に、素数ｑと、ビットサイズＬｅｎｑと、ｎ個の素数L_1、L_2、…、L_nと、ビットサイズＬｅｎＬとからなるパラメタ群を用いる。次に、２回めの素数生成の際に、素数ｑ’と、素数ｑ’のビットサイズＬｅｎｑ’と、ｊ個の２以外の小さな素数であるL_1'、L_2'、…、L_j'と、（$L_1' \times L_2' \times \cdots \times L_j'$）のビットサイズＬｅｎＬ’とからなるパラメタ群を用いるとしてもよい。

【００５３】ここで、素数ｑ≠素数ｑ’であり、ｎ≠ｊである。また、素数（L_1、L_2、…、L_n）≠素数（L_1'、L_2'、…、L_j'）である。これは、素数（L_1、L_2、…、L_n）と、素数（L_1'、L_2'、…、L_j'の少なくとも１個が異なっていることを示している。

（６）素数生成部１０１

素数生成部１０１は、図３に示すように、乱数生成部１３１、判定対象生成部１３２、第１素数判定部１３３、第２素数判定部１３４及び制御部１３５から構成されている。

【００５４】素数生成部１０１は、

$q = 1 \mod L_1$、

$q = 1 \mod L_2$、

…$q = 1 \mod L_n$を満たす素数ｑと、

素数ｑのビットサイズＬｅｎｑとが与えられたとき、素数ｑのビットサイズの２倍のビットサイズをもつ素数ｐを出力する。

【００５５】ここで、L_1、L_2、…、L_nは２以外の小さな素数である。また、（$L_1 \times L_2 \times \cdots \times L_n$）のビットサイズＬｅｎＬは予め与えられているものであるとする。小さな素数の例として、想定する入力ｑのビットサイズより小さな素数、例えば$L_1 = 3$、$L_2 = 5$などが挙げられる。

【００５６】（乱数生成部１３１）乱数生成部１３１は、生成制御部１０２からビットサイズＬｅｎｑ及びＬｅｎＬを受け取り、受け取ったビットサイズＬｅｎｑ及びＬｅｎＬを用いて、（Ｌｅｎｑ－ＬｅｎＬ－１）ビットサイズの乱数Ｒ’を生成し、生成した乱数Ｒ’を判定対象生成部１３２へ出力する。

【００５７】また、乱数生成部１３１は、第１素数判定部１３３から後述する第１判定情報を受け取る。また、第２素数判定部１３４から後述する第２判定情報を受け取る。乱数生成部１３１は、第１判定情報、又は第２判定情報を受け取ると、再度、受け取ったビットサイズＬｅｎｑ及びＬｅｎＬを用いて、（Ｌｅｎｑ－ＬｅｎＬ－１）ビットサイズの乱数Ｒ’を生成し、生成した乱数Ｒ’を判定対象生成部１３２へ出力する。

【００５８】（判定対象生成部１３２）判定対象生成部１３２は、生成制御部１０２から素数ｑを受け取り、乱数生成部１３１から乱数Ｒ’を受け取る。次に、判定対象生成部１３２は、受け取った素数ｑと乱数Ｒ’とを用いて、以下の式を満たす数Ｒと数Ｎとを生成する。

【００５９】

$R = L_1 \times L_2 \times \cdots \times L_n \times R'$

$N = 2 \times R \times q + 1$

次に、判定対象生成部１３２は、生成した数Ｒを第２素数判定部１３４へ出力し、生成した数Ｎを第１素数判定部１３３及び第２素数判定部１３４へ出力する。

【００６０】（第１素数判定部１３３）第１素数判定部１３３は、判定対象生成部１３２から数Ｎを受け取り、受け取った数Ｎを用いて、次に示す判定式１の成立を判定する。

$2^{N-1} = 1 \mod N$　　（判定式１）

判定式１が成立する場合には、その旨を示す第１判定情報を第２素数判定部１３４へ出力する。判定式１が成立しない場合には、その旨を示す第１判定情報を乱数生成部１３１へ出力する。

【００６１】（第２素数判定部１３４）第２素数判定部１３４は、判定対象生成部１３２から数Ｎと数Ｒとを受

け取り、また、第１素数判定部１３３から、判定式１が成立する旨を示す第１判定情報受け取る。判定式１が成立する旨を示す第１判定情報を受け取ると、次に、第２素数判定部１３４は、受け取った数Ｎと数Ｒとを用いて、次に示す判定式２の成立を判定する。

【００６２】

$2^{2R} \neq 1 \mod N$　（判定式２）

判定式２が成立する場合には、素数ｐとして数Ｎを生成制御部１０２へ出力する。判定式２が成立しない場合には、その旨を示す第２判定情報を乱数生成部１３１へ出力する。

（制御部１３５）制御部１３５は、素数生成部１０１を構成する各要素を制御する。

【００６３】（素数生成部１０１の動作の検証）第１素数判定部１３３及び第２素数判定部１３４による判定は、Pocklington判定である。Pocklington判定については、岡本　栄司、「暗号理論入門」、共立出版、1993,21ページ及び、A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, “Handbook of applied cryptography”, CRC Press, 1997, 144ページに詳しく述べられている。

【００６４】Ｎ＝２×Ｒ×ｑ＋１のｑが素数であり

$2^{N-1} = 1 \mod N$

$2^{2R} \neq 1 \mod N$

の両方が成り立つ場合、Ｎが素数になるので、素数生成部１０１は素数を出力する。また、乱数Ｒ’のビットサイズがＬｅｎｑ－ＬｅｎＬ－１であるので、数ＲのビットサイズがＬｅｎｑ－１になり、数Ｎのビットサイズが２×Ｌｅｎｑになる。

【００６５】（７）公開鍵生成部１０６

公開鍵生成部１０６は、素数記憶部１０３から素数p_a及び素数p_bを読み出し、読み出した素数p_aと素数p_bとを乗じて整数$n = p_a \times p_b$を算出し、算出した整数ｎを秘密鍵記憶部１０５及び公開鍵記憶部１０７へ書き込み、数（$p_a - 1$）と数（$p_b - 1$）との最小公倍数$L = LCM(p_a - 1, p_b - 1)$を算出する。

【００６６】また、公開鍵生成部１０６は、乱数生成部１０４から乱数ｅを受け取り、受け取った乱数ｅを用いて、数$d = e^{-1} \mod L$を算出し、算出した数ｄを秘密鍵記憶部１０５へ書き込み、乱数ｅを公開鍵記憶部１０７へ書き込む。

（８）乱数生成部１０４

乱数生成部１０４は、乱数ｅを生成し、生成した乱数ｅを公開鍵生成部１０６へ出力する。

【００６７】（９）送受信部１１４

送受信部１１４は、公開鍵記憶部１０７から整数ｎ及び乱数ｅを読み出し、読み出した整数ｎ及び乱数ｅをＰＣ３０へ出力する。また、送受信部１１４は、配信サーバ装置４０からインターネット６０及びＰＣ３０を介して、暗号文ｃを受信し、受信した暗号文ｃをメモリ部１０９内の一般領域１１１へ書き込む。

【００６８】（１０）復号部１０８

復号部１０８は、一般領域１１１から暗号文ｃを読み出し、秘密鍵記憶部１０５から数ｄ及び整数ｎを読み出し、読み出した数ｄ及び整数ｎを用いて、次の式により、暗号文ｃを復号して、復号文ｍ’を生成する。$m' = c^d \mod n$次に、復号部１０８は、生成した復号文ｍ’をメモリ部１０９内のセキュア領域１１０へ書き込む。

【００６９】（１１）認証部１１３

認証部１１３は、メモリカード１０が装着される相手の装置との間で、相手の装置の正当性を認証する。正当性が認証された場合に、メモリ部１０９内のセキュア領域１１０への情報の書き込み及びセキュア領域１１０からの情報の読み出しを許可する。

【００７０】（１２）制御部１１２

制御部１１２は、メモリカード１０を構成する各要素を制御する。１．３　ＰＣ３０ＰＣ３０は、図４に示すように、送受信部３０１、認証部３０２、制御部３０３、送受信部３０４、入力部３０５、表示部３０６から構成されている。

【００７１】この装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、液晶ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、前記装置は、その機能を達成する。

【００７２】ＰＣ３０は、メモリカード１０から整数ｎ及び乱数ｅを受け取り、受け取った整数ｎ及び乱数ｅを、インターネット６０を介して、配信サーバ装置４０へ送信する。また、ＰＣ３０は、配信サーバ装置４０から、インターネット６０を介して、暗号文ｃを受け取り、受け取った暗号文ｃを、メモリカード１０の送受信部１１４へ送信する。

【００７３】１．４　配信サーバ装置４０

配信サーバ装置４０は、図５に示すように、送受信部４０１、公開鍵記憶部４０２、暗号化部４０３、制御部４０４及び情報記憶部４０５から構成されている。この装置は、ＰＣ３０と同様に、コンピュータシステムであり、マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記装置は、その機能を達成する。

【００７４】（１）情報記憶部４０５

情報記憶部４０５は、あらかじめ平文ｍを記憶している。平文ｍは、具体的には、デジタルの音楽情報である。

（２）公開鍵記憶部４０２

公開鍵記憶部４０２は、公開鍵としての整数ｎ及び乱数ｅを記憶するための領域を備えている。

【００７５】（３）送受信部４０１
送受信部４０１は、ＰＣ３０からインターネット６０を介して、整数ｎ及び乱数ｅを受信し、受信した整数ｎ及び乱数ｅを公開鍵記憶部４０２へ書き込む。また、送受信部４０１は、暗号化部４０３から、暗号文ｃを受け取り、受け取った暗号文ｃを、インターネット６０を介して、ＰＣ３０へ送信する。
【００７６】（４）暗号化部４０３
暗号化部４０３は、情報記憶部４０５から平文ｍを読み出し、公開鍵記憶部４０２から整数ｎ及び乱数ｅを読み出し、読み出した整数ｎ及び乱数ｅを用いて、次の式により、平文ｍを暗号化して、暗号文ｃを生成する。$c = m^e \bmod n$次に、暗号化部４０３は、生成した暗号文ｃを送受信部４０１へ出力する。
【００７７】（５）制御部４０４
制御部４０４は、配信サーバ装置４０を構成する各要素を制御する。
１．５　ＰＤＡ２０及びヘッドフォン２１
ＰＤＡ２０は、メモリカード１０のメモリ部１０９内のセキュア領域１１０に書き込まれている復号文ｍ’を読み出し、読み出した復号文ｍ’をアナログの音声信号に変換し、音声信号をヘッドフォン２１へ出力する。
【００７８】ヘッドフォン２１は、音声信号を音声に変換して出力する。
１．６　携帯電話５０
携帯電話５０は、無線電波を用いて、他の電話機との間で通信を行うことができる携帯型の電話機としての構成を有し、さらに、ＰＣ３０及びＰＤＡ２０と同様の構成を有する。
【００７９】この携帯電話５０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、液晶ディスプレイユニット、入力部、通信部、マイク、スピーカなどから構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、携帯電話５０は、その機能を達成する。
【００８０】携帯電話５０は、ＰＣ３０と同様に、メモリカード１０から整数ｎ及び乱数ｅを受け取り、受け取った整数ｎ及び乱数ｅを、インターネット６０を介して、配信サーバ装置４０へ送信する。また、携帯電話５０は、配信サーバ装置４０から、インターネット６０を介して、暗号文ｃを受け取り、受け取った暗号文ｃを、メモリカード１０の送受信部１１４へ送信する。
【００８１】携帯電話５０は、ＰＤＡ２０と同様に、メモリカード１０に記憶されているデジタル著作物を変換して電気信号を生成し、生成した電気信号を音声に変換して、音声を出力する。
１．７　コンテンツ配信システム１の動作
（１）コンテンツ配信システム１の動作コンテンツ配信システム１の動作について、図６に示すフローチャートを用いて説明する。
【００８２】メモリカード１０の素数生成部１０１は、ランダムに素数p_a及び素数p_bを生成し、生成した素数p_a及び素数p_bを素数記憶部１０３へ書き込む（ステップＳ１０１）。次に、公開鍵生成部１０６は、素数記憶部１０３から素数p_a及び素数p_bを読み出し、読み出した素数p_aと素数p_bとを乗じて整数$n = p_a \times p_b$を算出し、算出した整数ｎを秘密鍵記憶部１０５及び公開鍵記憶部１０７へ書き込み、数（$p_a - 1$）と数（$p_b - 1$）との最小公倍数$L = LCM(p_a - 1, p_b - 1)$を算出する（ステップＳ１０２）。次に、乱数生成部１０４は、乱数ｅを生成し、生成した乱数ｅを公開鍵生成部１０６へ出力する（ステップＳ１０３）。次に、公開鍵生成部１０６は、乱数ｅを受け取り、受け取った乱数ｅを用いて、数$d = e^{-1} \bmod L$を算出し、算出した数ｄを秘密鍵記憶部１０５へ書き込み、乱数ｅを公開鍵記憶部１０７へ書き込む（ステップＳ１０４）。次に、送受信部１１４は、公開鍵記憶部１０７から整数ｎ及び乱数ｅを読み出し、読み出した整数ｎ及び乱数ｅをＰＣ３０へ出力し（ステップＳ１０５）、ＰＣ３０は、整数ｎ及び乱数ｅを、インターネット６０を介して、配信サーバ装置４０へ送信する（ステップＳ１０６）。
【００８３】配信サーバ装置４０の公開鍵記憶部４０２は、ＰＣ３０からインターネット６０及び送受信部４０１を介して、整数ｎ及び乱数ｅを、受信して記憶し（ステップＳ１０６）、暗号化部４０３は、情報記憶部４０５から平文ｍを読み出し、公開鍵記憶部４０２から整数ｎ及び乱数ｅを読み出し、読み出した整数ｎ及び乱数ｅを用いて、次の式により、平文ｍを暗号化して、暗号文ｃを生成する。
【００８４】$c = m^e \bmod n$　（ステップＳ１０７）次に、暗号化部４０３は、送受信部４０１及びインターネット６０を介して、暗号文ｃをＰＣ３０へ送信し（ステップＳ１０８）、ＰＣ３０は、暗号文ｃを受け取り、受け取った暗号文ｃを、メモリカード１０の送受信部１１４へ送信し、送受信部１１４は、受信した暗号文ｃをメモリ部１０９内の一般領域１１１へ書き込む（ステップＳ１０９）。復号部１０８は、一般領域１１１から暗号文ｃを読み出し、秘密鍵記憶部１０５から数ｄ及び整数ｎを読み出し、読み出した数ｄ及び整数ｎを用いて、次の式により、暗号文ｃを復号して、復号文ｍ’を生成する。$m' = c^d \bmod n$次に、復号部１０８は、生成した復号文ｍ’をメモリ部１０９内のセキュア領域１１０へ書き込む（ステップＳ１１０）。
【００８５】ＰＤＡ２０は、メモリカード１０のメモリ部１０９内のセキュア領域１１０に書き込まれている復号文ｍ’を読み出し（ステップＳ１１１）、読み出した

復号文m’をアナログの音声信号に変換し、音声信号をヘッドフォン２１へ出力する。ヘッドフォン２１は、音声信号を音声に変換して出力する（ステップＳ１１２）。

【００８６】なお、メモリカード１０における上記動作は、制御部１１２が、メモリカード１０を構成する各要素を制御することにより行われる。

（２）素数生成部１０１の動作

素数生成部１０１の動作について、図７に示すフローチャートを用いて説明する。

【００８７】乱数生成部１３１は、Ｌｅｎｑ－ＬｅｎＬ－１ビットの乱数Ｒ’を生成し、判定対象生成部１３２へ出力する（ステップＳ１３２）。次に、判定対象生成部１３２は、数Ｒと数Ｎとを計算し、数Ｎを第１素数判定部１３３へ出力し、数Ｎと数Ｒとを第２素数判定部１３４に出力する（ステップＳ１３３）。次に、第１素数判定部１３３は、2^{N-1} ＝１　ｍｏｄ　Ｎ（判定式１）の成立を判定し、成立しない場合は（ステップＳ１３４）、ステップＳ１３２へ戻って処理を繰り返す。

【００８８】成立する場合には（ステップＳ１３４）、第２素数判定部１３４は、2^{2R} ≠１ｍｏｄ　Ｎ（判定式２）の成立を判定し、成立しない場合は（ステップＳ１３５）、ステップＳ１３２へ戻って処理を繰り返す。成立する場合は（ステップＳ１３５）、素数として数Ｎを生成制御部１０２へ出力し、素数生成部１０１は、処理を終了する。

【００８９】なお、素数生成部１０１における上記動作は、制御部１３５が、素数生成部１０１を構成する各要素を制御することにより行われる。

１．８　計算量の評価

素数生成部１０１による計算量について説明する。以下において、L_1 ＝３、L_2 ＝５、L_3 ＝７、ｎ＝３、Ｌ＊ｅｎｑ＝２５６ビットとし、２×Ｌｅｎｑ＝５１２ビットの冪乗剰余演算における演算回数を見積もる。

$$(2-1)\times(3-1)\times(5-1)\times(7-1)/(2\times3\times5\times7)$$
$$=48/210$$
$$=8/35$$

となる。これは、従来例１と同じ確率である。

【００９３】次に、第１素数判定部１３３の判定を通過する確率は、Miller-Rabin判定を通過する確率と等しく、１／４以下である。従って、１つの合成数に対して行う冪乗剰余演算の回数は、１＋１／４以下である。当然、素数に対して行う冪乗剰余演算回数は、２である。以上より、２５６ビットの素数を用いて、５１２ビットの素数を生成するために行う５１２ビットの冪乗剰余演算回数は、

（１＋１／４）（（ｌｎ　2^{512} ）×８／３５－１）＋２＝８９．５

以下である。

【００９４】第１の実施の形態では、Ｌｅｎｑ＝２５６ビットの素数から、２×Ｌｅｎｑ＝５１２ビットの素数を生成するが、第１の実施の形態の素数生成部１０１を再帰的に使用することで、簡単に素数が分かる１６ビットの素数から、５１２ビットの素数を生成することができる。よって、１２８ビットから２５６ビットの素数を生成する場合も同様に考えると、２５６ビットの素数を生成するために行う２５６ビットの冪乗剰余演算回数は、

（１＋１／４）　（（ｌｎ　2^{256} ）×８／３５－１）＋２＝４５．１

以下である。

【００９５】冪乗剰余演算の計算量は、法のＮに依存し、Ｎの３乗のオーダである。従って、２５６ビットの冪乗剰余演算８回を、５１２ビットの冪乗剰余演算１回相当と考えられる。６４ビットから１２８ビットなどの他も同様に考えると第１の実施の形態の素数生成部１０１全体の計算量を、５１２ビットの冪乗剰余演算回数で

【００９０】一般に、数Ｒを任意に選ぶ場合、Ｒが素数となる確率は、１／（ｌｎ　Ｒ）程度であるので、この場合、５１２ビットの素数を生成するためにPocklington 判定を試す回数は、ｌｎ　（2^{512} ）と見積もることができる。ここで、ｌｎ　Ｒは、Ｒの自然対数である。

上記第１の実施の形態では、

$N=2\times R\times q+1$
$=2\times L_1\times L_2\times\cdots\times L_n\times R'\times q+1$

であるので、

$N=1 \mod 2$、
$N=1 \mod L_1$、
$N=1 \mod L_2$、
…、$N=1 \mod L_n$ であり、Ｎは、L_1、L_2、…、L_n のいずれでも割り切れない。

【００９１】ｍｏｄ　（$2\times L_1\times L_2\times\cdots\times L_n$）の数が、２、$L_1$、$L_2$、…、$L_n$で割り切れない確率は、

$\phi(2\times L_1\times L_2\times\cdots\times L_n)/(L_1\times L_2\times\cdots\times L_n)=(2-1)\times(L_1-1)\times(L_2-1)\times\cdots\times(L_n-1)/(2\times L_1\times L_2\times\cdots\times L_n)$

である。φは、オイラー関数と呼ばれ、辻井　重男、笠原　正雄、「暗号と情報セキュリティ」、昭晃堂、1990、11～12ページに詳しく説明されている。

【００９２】従って、Pocklington 判定を試す数の個数は、

$(2-1)\times(L_1-1)\times(L_2-1)\times\cdots\times(L_n-1)/(2\times L_1\times L_2\times\cdots\times L_n)$

倍に削減できる。ここで、

L_1 ＝３、L_2 ＝５、L_3 ＝７、ｎ＝３であるので、

見積もることができる。１６、３２ビットの素数生成の計算量は、６４、１２８、２５６、５１２ビットの素数生成の計算量に比べて小さいため無視し、第１の実施の形態１の素数生成部１０１全体の計算量を、５１２ビットの冪乗剰余演算回数で表すと、

$(1+1/4)\{((\ln 2^{64})\times 8/35-1)/512+((\ln 2^{128})\times 8/35-1)/64+((\ln 2^{256})\times 8/35-1)/8+((\ln 2^{512})\times 8/35-1)\}+2(1/512+1/64+1/8+1)=109.0$

以下である。

【００９６】これは、従来例１の１１６．８回以下と比べて、計算量が小さく、また、確定的に素数生成が可能になる。また、確定的な素数生成法である従来例２と比べて、２．２倍高速である。以上に説明したように、第１の実施の形態によると、従来例と比較すると、確定的な素数生成の計算時間を短縮できるという優れた効果がある。

【００９７】しかしながら、第１の実施の形態によると、

$N=1 \mod 2$、

$N=1 \mod L_1$、

$N=1 \mod L_2$、

‥$N=1 \mod L_n$ を満たす素数Nに限定して、素数生成を行うので、生成できる素数の種類が少ない。

【００９８】暗号への使用を考えると、素数の種類が限定されることは、暗号の使用法によっては、安全性の面で懸念される場合がある。次に示す第２の実施の形態は、この問題を解決することを目的としている。

２．第２の実施の形態

本発明に係る別の実施の形態としてのコンテンツ配信システム１ｂ（図示していない）について、説明する。

【００９９】コンテンツ配信システム１ｂは、コンテンツ配信システム１と同様に構成を有している。メモリカード１０は、素数生成部１０１に代えて、素数生成部１０１ｂを備えている。ここでは、コンテンツ配信システム１との相違点を中心として説明す。

２．１　メモリカード１０の生成制御部１０２

生成制御部１０２は、素数生成部１０１ｂへ、素数ｑと、素数ｑのビットサイズＬｅｎｑと、２以外の小さな素数であるL_1、L_2、‥、L_nと、($L_1\times L_2\times\cdots\times L_n$)のビットサイズＬｅｎＬと、$q \mod L_1$、$q \mod L_2$、‥、$q \mod L_n$とを出力し、次に、素数生成部１０１ｂから１個の素数ｐを受け取り、受け取った素数ｐを素数p_nとして素数記憶部１０３へ書き込む。

【０１００】次に、同様にして、素数生成部１０１ｂへ、素数ｑと、素数ｑのビットサイズＬｅｎｑと、２以外の小さな素数であるL_1、L_2、‥、L_nと、($L_1\times L_2\times\cdots\times L_n$)のビットサイズＬｅｎＬ、$q \mod L_1$、$q \mod L_2$、‥、$q \mod L_n$とを出力し、次に、素数生成部１０１ｂから１個の素数ｐを受け取り、受け取った素数ｐを素数p_nとして素数記憶部１０３へ書き込む。

【０１０１】２．２　メモリカード１０の素数生成部１０１ｂ

素数生成部１０１ｂは、素数ｑ、$q \mod L_1$、$q \mod L_2$、‥、$q \mod L_n$（L_1、L_2、‥、L_nは２以外の小さな素数）及び素数ｑのビットサイズＬｅｎｑが与えられた場合、素数ｑのビットサイズの２倍のビットサイズをもつ素数ｐを生成して出力する。

【０１０２】ここで、L_1、L_2、‥、L_n及び($L_1\times L_2\times\cdots\times L_n$)のビットサイズＬｅｎＬは予め与えられているものとする。また、小さな素数の例として、入力される素数ｑのビットサイズより小さな素数が挙げられる。素数生成部１０１ｂは、図８に示すように、部分情報設定部１３６ｂ、乱数生成部１３１ｂ、判定対象生成部１３２ｂ、第１素数判定部１３３ｂ、第２素数判定部１３４ｂ及び制御部１３５ｂから構成される。

【０１０３】（１）部分情報設定部１３６ｂ

部分情報設定部１３６ｂは、生成制御部１０２から素数ｑ、$q \mod L_1$、$q \mod L_2$、‥、$q \mod L_n$を受け取り、

$2\times u\times q+1\neq 0 \mod L_1$、

$2\times u\times q+1\neq 0 \mod L_2$、

‥$2\times u\times q+1\neq 0 \mod L_n$

を満たす数ｕを算出し、算出した数ｕを判定対象生成部１３２ｂへ出力する。

【０１０４】部分情報設定部１３６ｂの詳細について以下に説明する。部分情報設定部１３６ｂは、図８に示すように、整数生成部１４１ｂ及び情報合成部１４２ｂから構成される。

（整数生成部１４１ｂ）整数生成部１４１ｂは、乱数N_1（$1\leqq N_1\leqq L_1-1$）、N_2（$1\leqq N_2\leqq L_2-1$）、‥、N_n（$1\leqq N_n\leqq L_n-1$）を発生し、

$u_i=(N_i-1)/(2\times(q \mod L_i)) \mod L_i$

（$i=1、2、\cdots、n$）

を計算する。

【０１０５】次に、計算して得たu_i（$i=1、2、\cdots、n$）を情報合成部１４２ｂへ出力する。

（情報合成部１４２ｂ）情報合成部１４２ｂは、整数生成部１４１ｂからu_i（$i=1、2、\cdots、n$）を受け取り、受け取ったu_i（$i=1、2、\cdots、n$）を用いて、中国人の剰余定理から、

$u=u_i \mod L_i$　（$i=1、2、\cdots、n$）

を満たす$u \mod (L_1\times L_2\times\cdots\times L_n)$を求める。

【０１０６】ここで、中国人の剰余定理については、岡本　栄司、「暗号理論入門」、共立出版、１９９３、１０ページに詳しく述べられている。具体的には、情報合成部１４２ｂは、

$u'_2=((L_1)^{-1} \bmod L_2)\times((u_2-u_1) \bmod L_2)+u_1$

$u'_3=((L_1\times L_2)^{-1} \bmod L_3)\times((u_3-u'_2) \bmod L_3)+u'_2$

$\cdots u'_n=((L_1\times L_2\times\cdots\times L_{n-1})^{-1} \bmod L_n)\times((u_n-u'_{n-1}) \bmod L_n)+u'_{n-1}$

を計算し、ｕ＝ｕ’ｎ とする。

【０１０７】次に、情報合成部１４２ｂは、計算して得た数ｕを判定対象生成部１３２ｂへ出力する。（２）乱数生成部１３１ｂ

乱数生成部１３１ｂは、生成制御部１０２からＬｅｎｑ及びＬｅｎＬを受け取り、受け取ったＬｅｎｑ及びＬｅｎＬを用いて、（Ｌｅｎｑ－ＬｅｎＬ－１）ビット長の乱数Ｒ’を生成し、生成した乱数Ｒ’を判定対象生成部１３２ｂへ出力する。

【０１０８】また、乱数生成部１３１ｂは、第１素数判定部１３３ｂから後述する第３判定情報を受け取る。また、第２素数判定部１３４ｂから後述する第４判定情報を受け取る。乱数生成部１３１ｂは、第３判定情報、又は第４判定情報を受け取ると、再度、受け取ったビットサイズＬｅｎｑ及びＬｅｎＬを用いて、（Ｌｅｎｑ－ＬｅｎＬ－１）ビットサイズの乱数Ｒ’を生成し、生成した乱数Ｒ’を判定対象生成部１３２ｂへ出力する。

【０１０９】（３）判定対象生成部１３２ｂ

判定対象生成部１３２ｂは、生成制御部１０２から素数ｑ、L_1、L_2、$\cdots$、L_nを受け取り、部分情報設定部１３６ｂから数ｕを受け取り、乱数生成部１３１ｂから乱数Ｒ’を受け取る。次に、受け取った素数ｑ、L_1、L_2、$\cdots$、L_n、数ｕ及び乱数Ｒ’を用いて、以下の式を満たす数Ｒ及び数Ｎを生成する。

【０１１０】

$R=u+L_1\times L_2\times\cdots\times L_n\times R'$

$N=2\times R\times q+1$

次に、判定対象生成部１３２ｂは、生成した数Ｒ及び数Ｎを第２素数判定部１３４ｂへ出力し、生成した数Ｎを第１素数判定部１３３ｂへ出力する。（４）第１素数判定部１３３ｂ第１素数判定部１３３ｂは、判定対象生成部１３２ｂから数Ｎを受け取り、受け取った数Ｎを用いて、次の判定式３が成立するか否かを判定する。

【０１１１】$2^{N-1}=1 \bmod N$　　（判定式３）

判定式３が成立する場合には、第１素数判定部１３３ｂは、成立する旨を示す第３判定情報を第２素数判定部１３４ｂへ出力する。判定式３が成立しない場合には、成立しない旨を示す第３判定情報を乱数生成部１３１ｂへ出力する。

（５）第２素数判定部１３４ｂ

第２素数判定部１３４ｂは、判定対象生成部１３２ｂから数Ｒ及び数Ｎを受け取る。また、第１素数判定部１３３ｂから判定式３が成立する旨を示す第３判定情報を受け取る。

【０１１２】第３判定情報を受け取ると、第２素数判定部１３４ｂは、受け取った数Ｒ及び数Ｎを用いて、次の判定式４が成立するか否かを判定する。

$2^{2R}\neq 1 \bmod N$　　（判定式４）

判定式４が成立する場合には、第２素数判定部１３４ｂは、数Ｎを素数ｐとして生成制御部１０２へ出力する。

【０１１３】判定式４が成立しない場合には、第２素数判定部１３４ｂは、判定式４が成立しない旨を示す第４判定情報を乱数生成部１３１ｂへ出力する。

（６）制御部１３５ｂ

制御部１３５ｂは、素数生成部１０１ｂを構成する各要素を制御する。

２．３　素数生成部１０１ｂの検証

第１素数判定部１３３ｂ及び第２素数判定部１３４ｂは、それぞれ素数生成部１０１の第１素数判定部１３３及び第２素数判定部１３４と同じであるので、素数生成部１０１ｂは、素数生成部１０１と同様、素数を出力する。

【０１１４】また、乱数Ｒ’のビットサイズがＬｅｎｑ－ＬｅｎＬ－１であるので、ＲのビットサイズがLen_q-1になり、Ｎのビットサイズが２×Ｌｅｎｑになる。

２．４　素数生成部１０１ｂの動作

素数生成部１０１ｂの動作について図９に示すフローチャートを用いて説明する。

【０１１５】部分情報設定部１３６ｂは、$2\times u\times q+1\neq 0 \bmod (L_1\times L_2\times\cdots\times L_n)$を満たすｕを計算し、計算したｕを判定対象生成部１３２ｂへ出力する（ステップＳ１５２）。次に、乱数生成部１３１ｂは、Ｌｅｎｑ－ＬｅｎＬ－１ビットの乱数Ｒ’を生成し、生成した乱数Ｒ’を判定対象生成部１３２ｂへ出力する（ステップＳ１５３）。判定対象生成部１３２ｂは、ＲとＮを計算し、Ｎを第１素数判定部１３３ｂへ出力し、ＮとＲを第２素数判定部１３４ｂへ出力する（ステップＳ１５４）。第１素数判定部１３３ｂは、判定式３の成立を判定し、成立しない場合は（ステップＳ１５５）、ステップＳ１５３へ戻って処理を繰り返す。

【０１１６】成立する場合は（ステップＳ１５５）、第２素数判定部１３４ｂは、判定式４の成立を判定し、成立しない場合は（ステップＳ１５６）、ステップＳ１５３へ戻って処理を繰り返す。成立する場合は（ステップＳ１５６）、第２素数判定部１３４ｂは、素数ｐとして数Ｎを生成制御部１０２へ出力し（ステップＳ１５７）、素数生成部１０１ｂは、処理を終了する。

【０１１７】２．４　計算量の評価と効果

計算量については、第１の実施の形態とほぼ同じである。ただし、第１の実施の形態の計算量と比べて、部分

情報設定部１３６ｂの計算量のみが増加する。しかし、部分情報設定部１３６ｂは、ｍｏｄ　L_1、ｍｏｄL_2、…、ｍｏｄ　L_nの計算、及び中国人の剰余定理の計算のみであり、２×Ｌｅｎｑビットの数の計算と比較して、小さくほとんど０とみなしても問題ない。

【０１１８】従って、第２の実施の形態について、計算量に関し、第１の実施の形態と同等の効果が望める。また、$N=N_1 \mod L_1$、$N_2 \mod L_2$、…、$N_n \mod L_n$であり、N_1、N_2、…、N_nは乱数であるので、素数生成部１０１ｂは、生成する素数を限定しない。そのため、素数が限定されることによる安全性の懸念がなくなる。

【０１１９】従って、素数生成部１０１ｂによると、（１）生成する素数を限定しない、（２）確定的な素数を生成する、（３）従来例と比較して高速に素数を生成するという優れた効果がある。以上に説明したように第２の実施の形態によると、従来例と比較して、確定的な素数生成の計算時間を短縮でき、さらに、生成する素数の種類を限定しないため、素数を限定することによる安全性の懸念がなくなり、安全性の面でもよい。このことから、高速な暗号方式や署名方式を可能にする素数生成部を提供することができ，その実用的価値は大きい。

【０１２０】３．変形例

第１の実施の形態、又は第２の実施の形態においてそれぞれ説明した素数生成を適用する暗号通信システム（図示していない）について説明する。暗号通信システムは、管理センタ装置、ユーザＡ装置及びユーザＢ装置から構成される。管理センタ装置、ユーザＡ装置及びユーザＢ装置は、それぞれ、相互にネットワークを介して接続されている。

【０１２１】管理センタ装置は、内部に、第１の実施の形態に示す生成制御部１０２及び素数生成部１０１を備え、生成制御部１０２及び素数生成部１０１により２個の素数p_a及び素数p_bを生成する。なお、管理センタ装置は、内部に、第２の実施の形態に示す生成制御部１０２及び素数生成部１０１ｂを備えるとしてもよい。以下に、暗号通信システムの動作について、図１０に示すフローチャートを用いて説明する。ここでは、素因数分解することが計算量上困難であることを安全性の根拠とするＲＳＡ暗号を応用している。ＲＳＡ暗号については、岡本　龍明、山本　博資、「現代暗号」、産業図書、１９９７、１１０～１１３ページが詳しく説明されている。

【０１２２】（１）管理センタ装置による公開鍵の生成

管理センタ装置は、生成制御部１０２及び素数生成部１０１により、ランダムに素数p_a及び素数p_bを生成し（ステップＳ１７１）、素数p_a及び素数p_bを用いて、$n=p_a \times p_b$、及び$L=LCM(p_a-1, p_b-1)$を計算する（ステップＳ１７２）。

【０１２３】次に、管理センタ装置は、ランダムに乱数ｅ（$1 \leqq e \leqq L-1$，$GCD(e, L)=1$）を発生させ、$d=e^{-1} \mod L$を計算する（ステップＳ１７３）。ここで、ＧＣＤ（ｅ，Ｌ）は、ｅとＬの最大公約数である。その後、管理センタ装置は、素数p_a、素数p_b及び数ｄを秘密鍵として、ユーザＡ装置に対して秘密裏に送信し（ステップＳ１７４）、ユーザＢ装置に対して、数ｎ及び数ｅをユーザＡ装置の公開鍵として公開して送信する（ステップＳ１７５）。

【０１２４】（２）ユーザＢ装置による暗号文の生成

ユーザＢ装置は、$c=m^e \mod n$を計算する（ステップＳ１７６）。ここで、ｍは、ユーザＢ装置がユーザＡ装置へ送信するメッセージである。次に、ユーザＢ装置は、得られたｃを暗号文として、ユーザＡ装置に送信する（ステップＳ１７７）。

【０１２５】（３）ユーザＡ装置による暗号文の復号

ユーザＡ装置は、$m'=c^d \mod n$を計算して、復号メッセージｍ’を得る（ステップＳ１７８）。ここで、

$$c^d=(m^e)^d \mod n$$
$$=m^{**}(e \times d \mod L) \mod n$$
$$=m^1 \mod n$$
$$=m \mod n$$

となることから、メッセージｍが復号メッセージｍ’と同一であることは明らかである。

【０１２６】以上説明したように、公開鍵の生成のステップＳ１７１において、素数生成が行われる。この素数生成のステップにおいて、第１の実施の形態又は第２の実施の形態に示す生成制御部及び素数生成部が用いられるので、第１の実施の形態又は第２の実施の形態において説明した効果が得られる。

【０１２７】４．まとめ

以上説明したように、素数ｑと２以外の前記素数ｑより小さな素数L_1、L_2、…、L_n（$n \geqq 2$）とを入力とし、前記素数ｑより大きな素数Ｎを出力する素数生成部は、素数ｑが、$q=1 \mod L_i$（$i=1, 2, \cdots, n$）を満たし、$N=1 \mod L_i$（$i=1, 2, \cdots, n$）を満たすＮを素数として生成する。

【０１２８】また、素数生成部は、乱数Ｒ’を生成し、前記素数ｑと前記乱数Ｒ’から、$R=L_1 \times L_2 \times \cdots \times L_n \times R'$と、$N=2 \times R \times q+1$とを生成し、生成した前記Ｎ及び前記Ｒを用いて、前記Ｎの素数判定を行う。また、素数ｑと２以外の前記素数ｑより小さな素数L_1、L_2、…、L_n（$n \geqq 2$）を入力とし、前記素数ｑより大きな素数Ｎを出力する素数生成部は、$2 \times u \times q+1 \neq 0 \mod L_i$（$i=1, 2, \cdots, n$）を満たすｕを出力し、乱数Ｒ’を生成し、生成した前記ｕ及び前記乱数Ｒ’を用いて、$R=u+L_1 \times L_2 \times \cdots \times L_n \times R'$と、$N=2 \times R \times q+1$とを出力し、前記Ｎ及び前記Ｒを用いて、前記Ｎの素数判定を行う。

【０１２９】また、前記素数生成部は、整数N_i（$1 \leqq$

$N_1 \leqq L_1 - 1$）、N_2（$1 \leqq N_2 \leqq L_2 - 1$）、…、$N_n$（$1 \leqq N_n \leqq L_n - 1$）を発生し、$u_i = (N_i - 1) / (2 \times (q \bmod L_i)) \bmod L_i$（$i = 1, 2, \cdots, n$）を計算し、前記$u_i$（$i = 1, 2, \cdots, n$）を用いて、$u = u_i \bmod L_i$（$i = 1, 2, \cdots, n$）を満たすuを計算する。

【０１３０】また、前記素数判定部は、前記Nに対し、$2^{N-1} = 1 \bmod N$の成立を判定し、前記N及びRに対し、$2^{2R} \neq 1 \bmod N$の成立を判定する。このように、本発明によると、確定的な素数生成ができるとともに、従来例と比較して、計算時間を短縮できる。また、生成する素数の種類を限定しないようにできるので、素数を限定することによる安全性の懸念がなくなり、安全性の面でもよい。

【０１３１】以上により、高速な暗号方式や署名方式を可能にする情報セキュリティ装置及び素数生成装置を提供することができ，その実用的価値は大きい。

５．その他の変形例

以上、実施の形態に基づいて説明したが、本発明はこれらの実施の形態に限られないことは勿論である。次のように構成してもよい。

【０１３２】（１）本発明は、本実施の形態に示す素数生成部により、整数Ｌｅｎを入力とし、Ｌｅｎビットの素数を出力するとしてもよい。

（２）上記において説明した素数生成部は、独立した１個の装置であるとしてもよい。

（３）本発明は、本実施の形態に示す素数生成部を備える素数応用装置であるとしてもよい。素数応用装置の具体的な例は、暗号化装置及び暗号復号装置からなる暗号通信システム、デジタル署名作成装置及び署名検証装置からなるデジタル署名システムである。これらのシステムは、情報を安全かつ確実に扱う情報セキュリティシステムである。

【０１３３】（４）第１素数判定部１３３、第２素数判定部１３４、第１素数判定部１３３ｂ、第２素数判定部１３４ｂは、上記実施の形態と異なる素数判定式を使用するとしてもよい。例えば、第１素数判定部１３３及び第１素数判定部１３３ｂは、次の判定式を用いるとしてもよい。

【０１３４】$a^{N-1} = 1 \bmod N$

としてもよい。但し、aは$1 \leqq a \leqq N-1$を満たす整数である。また、第２素数判定部１３４及び第２素数判定部１３４ｂは、つぎの判定式を用いるとしてもよい。

$b^{2R} \neq 1 \bmod N$

又は、

$GCD(b^{2R} - 1, N) = 1$

としてもよい。但し、bは$1 \leqq b \leqq N-1$を満たす整数である。

【０１３５】（５）デジタル著作物は、音楽であるとしているが、その他のデジタル情報であるとしてもよい。例えば、音声、動画像、静止画像、文章、表形式のデータ、コンピュータプログラムなどのデジタル情報であるとしてもよい。

（６）上記の実施の形態において、ＲＳＡ暗号を適用するセキュリティシステムにおける素数生成部について説明しているが、素数生成部の利用は、ＲＳＡ暗号を適用するセキュリティシステムに限定されるものではない。例えば、楕円暗号において、素数生成部を適用することが可能である。楕円暗号では、１個の素数を生成して用いる。

【０１３６】（７）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ―ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０１３７】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【０１３８】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（７）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０１３９】

【発明の効果】上記目的を達成するために、素因数分解をすることが計算量の上で困難であることを根拠として、２個の素数を生成し生成した２個の素数の乗算を用いて、所定の情報を安全かつ確実に扱い、各素数生成の際に、既知の素数ｑの２倍のビット長を有する素数Ｎを生成する情報セキュリティ装置であって、素数ｑ及びｎ個の素数L_1、L_2、・・・、L_nを取得し、ここで、素数L_1、L_2、・・・、L_nは、それぞれ素数ｑより小さい２以外の素数であり、素数ｑは、$q = 1 \bmod L_i$（$i = 1, 2, \cdots, n$）を満たす取得手段と、取得した前記素数L_1、L_2、・・・、L_nに係る

数を除外した選択により、取得した前記素数ｑの２倍のビット長を有する数Ｎを生成する生成手段と、生成した数Ｎの素数判定を行い、数Ｎが素数であると判定とされた場合に、数Ｎを素数として出力する判定手段とを備える。

【０１４０】この構成によると、確定的な素数生成ができるとともに、従来と比較して、計算時間を短縮できる。また、前記生成手段は、Ｎ＝１　ｍｏｄ　L_i　（ｉ＝１、２、・・・、ｎ）を満たす前記数Ｎを生成する。また、前記生成手段は、（Ｌｅｎｑ－ＬｅｎＬ－１）ビット長の乱数Ｒ’を生成し、ここで、Ｌｅｎｑは、素数ｑのビット長であり、ＬｅｎＬは、（$L_1 \times L_2 \times \cdots \times L_n$）のビット長である乱数生成部と、生成したＲ’及び前記素数L_1、L_2、・・・、L_nを用いて、数$R = L_1 \times L_2 \times \cdots \times L_n \times R'$により、数Ｒを生成し、取得した素数ｑ及び生成した数Ｒを用いて、数Ｎ＝２×Ｒ×ｑ＋１を生成する判定対象生成部とを含み、前記判定手段は、前記数Ｎ及び前記数Ｒを用いて、前記数Ｎの素数判定を行う。

【０１４１】この構成によると、計算時間を短縮できる。また、前記生成手段は、取得した前記素数ｑを用いて、$2 \times u \times q + 1 \neq 0 \bmod L_i$　（ｉ＝１、２、・・・、ｎ）　を満たす数ｕを生成する部分情報生成部と、乱数Ｒ’を生成する乱数生成部と、取得した前記素数L_1、L_2、・・・、L_nと、生成した前記数ｕと、生成した前記乱数Ｒ’を用いて、$R = u + L_1 \times L_2 \times \cdots \times L_n \times R'$により、数Ｒを生成し、取得した前記素数ｑと、生成した数Ｒとを用いて、Ｎ＝２×Ｒ×ｑ＋１により、数Ｎを生成する判定対象生成部とを含み、前記判定手段は、前記数Ｎ及び前記数Ｒを用いて、前記数Ｎの素数判定を行う。

【０１４２】この構成によると、生成する素数の種類を限定することなく、計算時間を短縮できる。

【図面の簡単な説明】

【図１】コンテンツ配信システム１の構成を示すブロック図である。

【図２】メモリカード１０の構成を示すブロック図である。

【図３】素数生成部１０１の構成を示すブロック図である。

【図４】ＰＣ３０の構成を示すブロック図である。

【図５】配信サーバ装置４０の構成を示すブロック図である。

【図６】コンテンツ配信システム１の動作を示すフローチャートである。

【図７】素数生成部１０１の動作を示すフローチャートである。

【図８】素数生成部１０１ｂの構成を示すブロック図である。

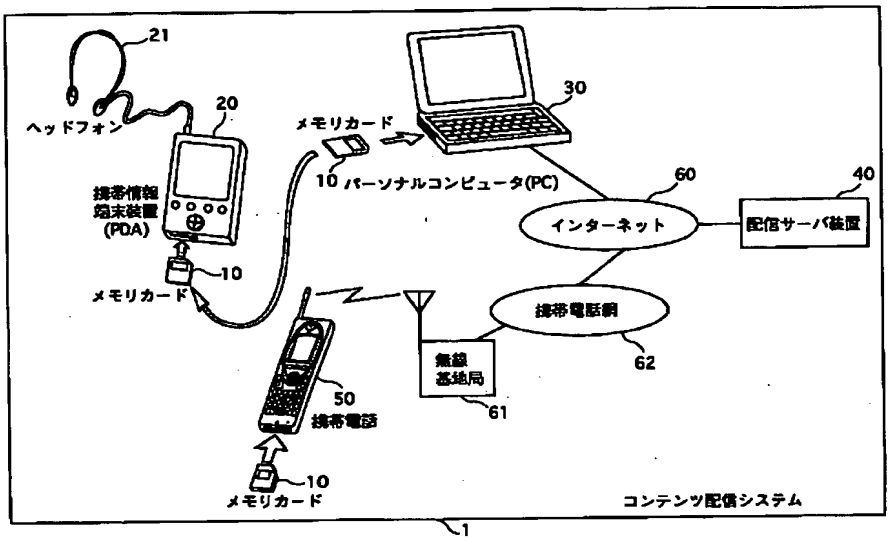
【図９】素数生成部１０１ｂの動作を示すフローチャートである。

【図１０】暗号通信システムの動作を示すフローチャートである。

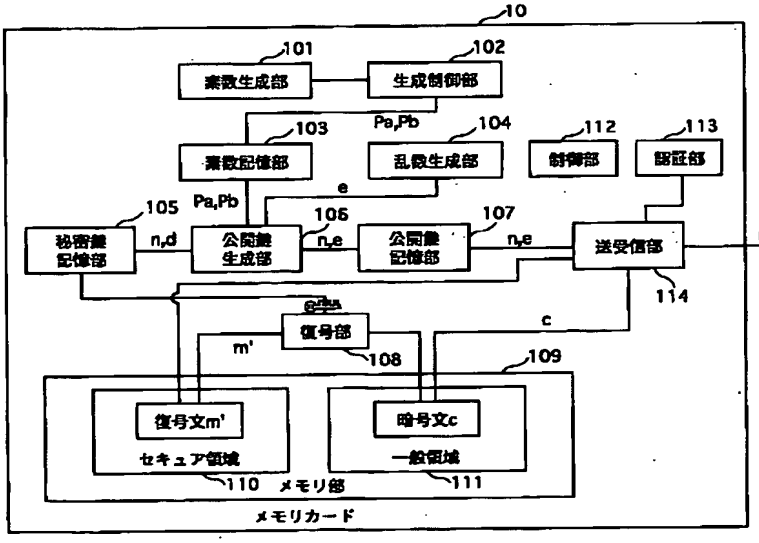
【符号の説明】

１　コンテンツ配信システム
１０　メモリカード
２０　ＰＤＡ
２１　ヘッドフォン
３０　ＰＣ
４０　配信サーバ装置
５０　携帯電話
６０　インターネット
６１　無線基地局
６２　携帯電話網
１０１　素数生成部
１０２　生成制御部
１０３　素数記憶部
１０４　乱数生成部
１０５　秘密鍵記憶部
１０６　公開鍵生成部
１０７　公開鍵記憶部
１０８　復号部
１０９　メモリ部
１１０　セキュア領域
１１１　一般領域
１１２　制御部
１１３　認証部
１１４　送受信部
１３１　乱数生成部
１３２　判定対象生成部
１３３　第１素数判定部
１３４　第２素数判定部
１３５　制御部

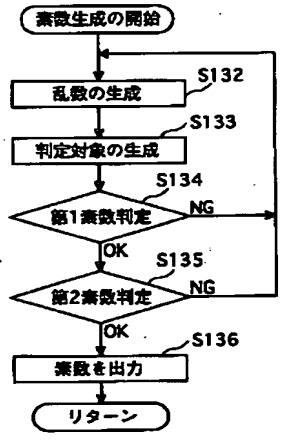
【図１】


21
ヘッドフォン
20
携帯情報端末装置(PDA)
10
メモリカード
メモリカード
10
パーソナルコンピュータ(PC)
30
60
インターネット
40
配信サーバ装置
携帯電話網
62
無線基地局
61
50
携帯電話
10
メモリカード
コンテンツ配信システム
1

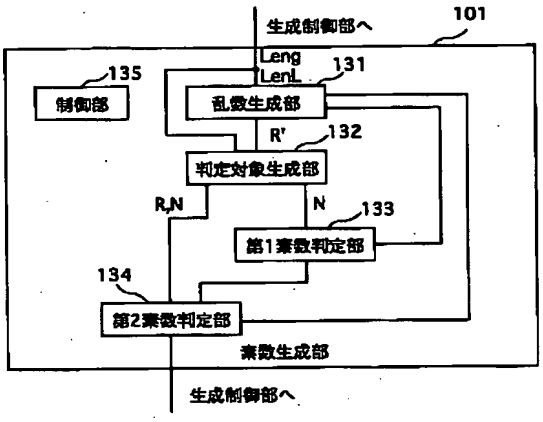
【図２】


10
101
素数生成部
102
生成制御部
Pa,Pb
103
素数記憶部
104
乱数生成部
112
制御部
113
認証部
e
105
Pa,Pb
秘密鍵記憶部
n,d
106
公開鍵生成部
n,e
107
公開鍵記憶部
n,e
送受信部
114
n,e,c
m'
PCへ又はPDAへ
c
復号部
m'
108
109
復号文m'
セキュア領域
暗号文c
一般領域
110
メモリ部
111
メモリカード

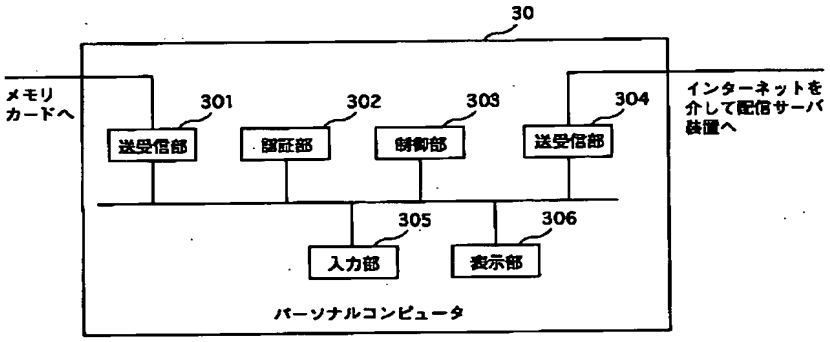
【図７】


素数生成の開始
乱数の生成
S132
判定対象の生成
S133
第1素数判定
S134
NG
OK
第2素数判定
S135
NG
OK
素数を出力
S136
リターン

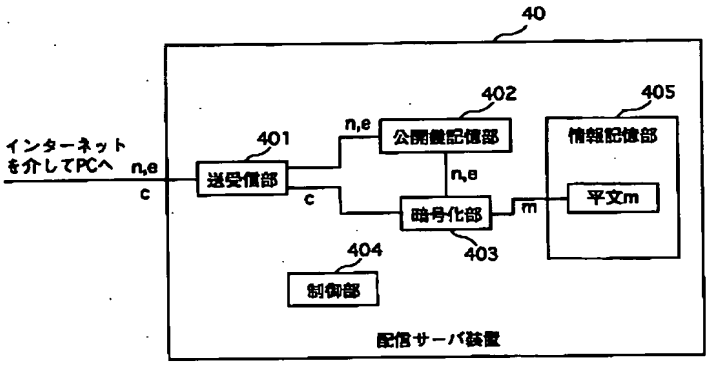
【図３】


生成制御部へ
101
Leng
Lenl
131
135
制御部
乱数生成部
R'
132
判定対象生成部
R,N
N
133
第1素数判定部
134
第2素数判定部
素数生成部
生成制御部へ

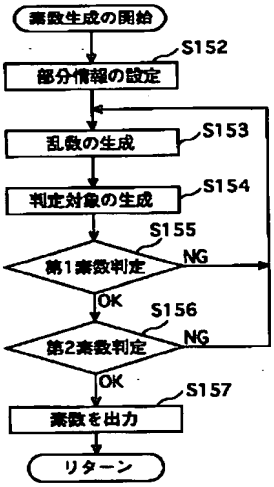
【図４】


30
メモリ
カードへ
301
302
303
304
インターネットを
介して配信サーバ
装置へ
送受信部
認証部
制御部
送受信部
305
306
入力部
表示部
パーソナルコンピュータ

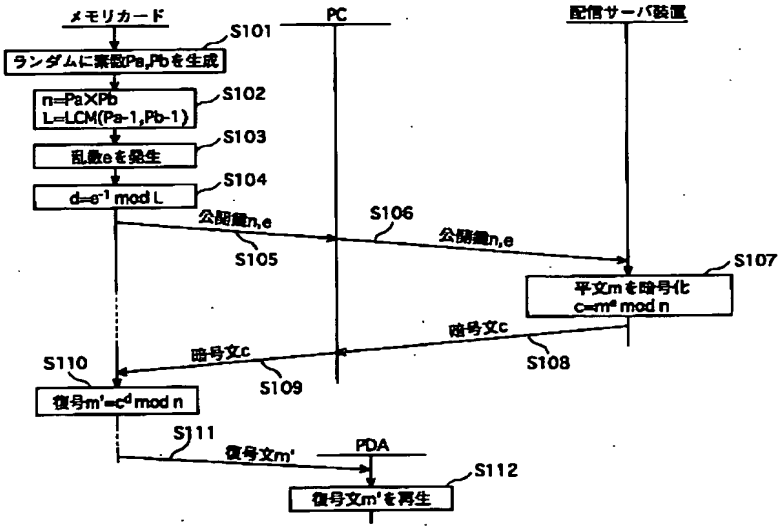
【図５】


40
インターネット
を介してPCへ
n,e
c
401
送受信部
n,e
公開鍵記憶部
402
c
暗号化部
403
n,e
m
405
情報記憶部
平文m
404
制御部
配信サーバ装置

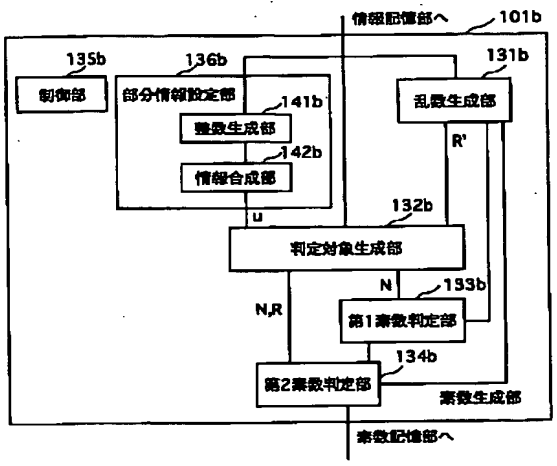
【図９】


素数生成の開始
S152
部分情報の設定
S153
乱数の生成
S154
判定対象の生成
S155
第1素数判定
NG
OK
S156
第2素数判定
NG
OK
S157
素数を出力
リターン

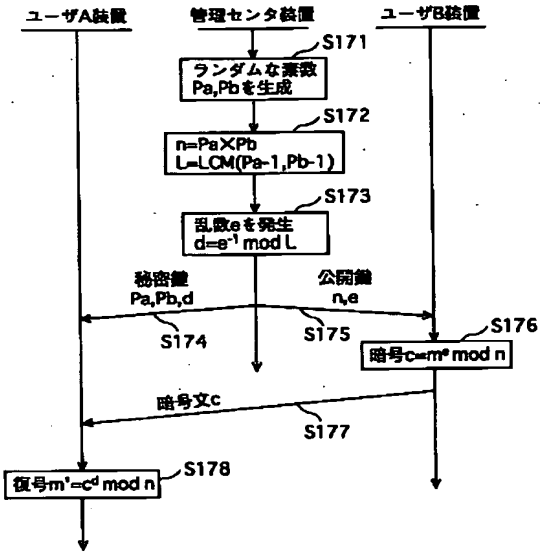
【図６】


メモリカード
PC
配信サーバ装置
S101
ランダムに素数Pa,Pbを生成
n=Pa×Pb
L=LCM(Pa-1,Pb-1)
S102
乱数eを発生
S103
d=e^-1 mod L
S104
公開鍵n,e
S105
S106
公開鍵n,e
S107
平文mを暗号化
c=m^e mod n
暗号文c
S108
暗号文c
S109
S110
復号m'=c^d mod n
S111
復号文m'
PDA
S112
復号文m'を再生

【図８】



【図１０】



フロントページの続き

(72)発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器
産業株式会社内

Ｆターム(参考)　5J104 AA23 EA04 EA19 EA32 JA28
NA02 NA18 NA35